Fundamental Properties of On-Off Transmission Scheme for Wiretap Channels

Shihao Yan†, Nan Yang†, and Jinhong Yuan‡
† Research School of Engineering, Australia National University, Canberra, ACT, Australia
‡ School of Electrical Engineering and Telecommunications, The University of New South Wales, Sydney, NSW, Australia
Email: shihao.yan@anu.edu.au, nan.yang@anu.edu.au, j.yuan@unsw.edu.au

***Abstract*—This work reveals some fundamental properties of an on-off transmission (OOT) scheme, in which a transmitter sends signals occasionally as per the capacity of the main channel in order to achieve physical layer security. To this end, we first identify the widely used hybrid secrecy outage probability as a function of the transmission probability and the conditional secrecy outage probability of the OOT scheme. This indicates, for the first time, that the hybrid secrecy outage probability can be achieved by the OOT scheme. We then derive a lower bound on the conditional secrecy outage probability of the OOT scheme in case of transmission, which is solely determined by the average signal-to-noise ratios (SNRs) of the main channel and eavesdropper's channel. Finally, we re-investigate the OOT scheme within an absolutely completely passive eavesdropping scenario, in which even the average SNR of the eavesdropper's channel is not required. Specifically, we derive an easy-evaluated expression for the average conditional secrecy outage probability of the OOT scheme by adopting an annulus threat model.**

I. Introduction

As wireless services become increasingly ubiquitous, a growing amount of research effort has been devoted to physical layer security in wireless networks [1–3]. This is mainly due to the fact that physical layer security can guarantee information secrecy regardless of the eavesdropper's computational capability and does not require the key distribution and management of traditional cryptographic techniques. In pioneering studies [4–6], a wiretap channel was characterized as the fundamental system model to protect information at the physical layer in wireless communications. In the wiretap channel, an eavesdropper (Eve) attempts to wiretap the communication between a transmitter (Alice) and an intended receiver (Bob). It was proved that perfect secrecy can be achieved when the capacity of the main channel between Alice and Bob is greater than the capacity of the eavesdropper's channel between Alice and Eve and both these two capacities are known to Alice.

In practical wiretap channels, the capacity of the eavesdropper's channel is hard to known at Alice since Eve is generally passive and does not send back its channel state information (CSI) to Alice. In the scenario without the CSI of the eavesdropper's channel, it is impossible to guarantee perfect secrecy and the secrecy outage probability, $\Pr(C_s < R_s)$, is widely adopted as the performance metric, where C_s is the secrecy capacity and R_s is the secrecy rate [7]. As pointed out by [8], $\Pr(C_s < R_s)$ includes the transmission outage probability and the conditional secrecy outage probability. As such, throughout this work we refer to $\Pr(C_s < R_s)$ as the *hybrid secrecy outage probability*. The hybrid secrecy outage probability is widely used as a key performance metric to evaluate and design techniques in the context of physical layer security in the literature. For example, the antenna selection techniques with and without space time coding schemes were examined by using $\Pr(C_s < R_s)$ as the primary performance metric [9–11]. In these studies, this hybrid secrecy outage probability was also adopted as the optimization criterion. In addition, the benefits of full-duplex transceivers in wiretap channels were evaluated by using $\Pr(C_s < R_s)$ as the performance metric [12, 13]. However, it has never been clarified which practical transmission scheme can achieve this hybrid secrecy outage probability. This leaves an important gap in our understanding on the wiretap channels and one of the objects of this work is to close this gap.

One widely adopted assumption in the context of physical layer security is that the average signal-to-noise ratio (SNR) of the eavesdropper's channel is known to Alice (e.g., [9–11, 13]). One reasonable justification of this assumption is that Eve can be a legitimate user that severed by Alice in the previous time slots (relatively to the time slots of interest for secure transmissions) and the average SNR of the eavesdropper's channel can be estimated based on the previous CSI. This justification may be unapplicable to some scenarios, e.g., Eve is a new user or Eve is moving fast within the network. In order to release this assumption, an annulus threat model was proposed in [14], in which Eve's location is uniformly distributed within the annulus bounded by two concentric circles. The authors of [14] examined the performances of an adaptive transmission scheme and a fixed-rate transmission scheme within the annulus threat model. Besides these two schemes, another important transmission scheme in the context of physical layer security is the on-off transmission (OOT) scheme, in which Alice sets R_s as a constant and only transmits signals when the capacity of the main channel is larger than R_s. The behaviors of this OOT scheme were not investigated within the annulus threat model and another purpose of this work is to examine the performance of the OOT scheme within the annulus threat model.

In this work, we explicitly prove that the hybrid secrecy outage probability can be achieved by the OOT scheme and we express the hybrid secrecy outage probability as a function of the transmission probability and the conditional secrecy

outage probability of the OOT scheme. We also reveal a counterintuitive property of the OOT scheme, which is that we cannot achieve an arbitrary small conditional secrecy outage probability by varying R_s. Furthermore, we derive an lower bound on the conditional secrecy outage probability of the OOT scheme, which is solely determined by the average SNRs of the main channel and the eavesdropper's channel. Finally, we derive the average conditional secrecy outage probability of the OOT scheme within the annulus threat model, based on which we examine the behaviors of this scheme in an completely passive eavesdropping scenario.

II. System Model

The wiretap channel of interest is illustrated in Fig. 1, where Eve attempts to intercept the communication between Alice and an Bob. Focusing on exploring the properties of the OOT scheme, we assume that Alice, Bob, and Eve are all equipped with a single antenna in this work. We also assume that the main channel and the eavesdropper's channel are subject to independent quasi-static Rayleigh fading with equal block length. As we will show later, Alice requires the capacity of the main channel to apply the OOT scheme. We adopt a practical assumption that Alice does not own the capacity of the eavesdropper's channel. We consider two passive eavesdropping scenarios: (i) the average SNR of the eavesdropper's channel is available at Alice and (ii) the average SNR of the eavesdropper's channel is unavailable at Alice but her location is uniformly distributed within an annulus.

The received signal at Bob is

$$y_B = hx + n_B, \tag{1}$$

where h denotes the complex gain of the main channel, x is the transmit signal, and n_B is the Gaussian noise of the main channel with zero mean and variance σ_B^2. Considering the transmit power constraint and denoting Alice's total transmit power as P_A, we have $\mathbb{E}[|x|^2] = P_A$. Based on (1), the instantaneous SNR at Bob is given by

$$\gamma_B = \frac{|h|^2 P_A}{\sigma_B^2} = \overline{\gamma}_B |h|^2, \tag{2}$$

where $\overline{\gamma}_B = P_A/\sigma_B^2$ denotes the average SNR of the main channel. The cumulative distribution function (cdf) of γ_B is given by

$$F_{\gamma_B}(\gamma_B) = 1 - e^{-\frac{\gamma_B}{\overline{\gamma}_B}}. \tag{3}$$

The received signal signal at Eve is given by

$$y_E = gx + n_E, \tag{4}$$

where g is the eavesdropper's channel gain and n_E is the Gaussian noise of the eavesdropper's channel with zero mean and variance σ_E^2. The instantaneous SNR at Eve after is given by

$$\gamma_E = \frac{|g|^2 P_A}{\sigma_E^2} = \overline{\gamma}_E |g|^2, \tag{5}$$

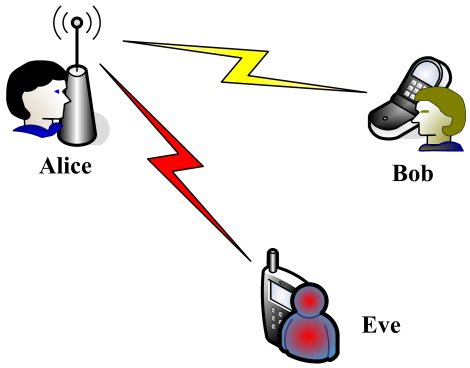

Fig. 1. Illustration of the wiretap channel of interest.

where $\overline{\gamma}_E = P_A/\sigma_E^2$ is the average SNR of the eavesdropper's channel. Then, the probability density function (pdf) of γ_E is given by [15]

$$f_{\gamma_E}(\gamma_E) = \frac{1}{\overline{\gamma}_E} e^{-\frac{\gamma_E}{\overline{\gamma}_E}}, \tag{6}$$

and the cdf of γ_E is given by

$$F_{\gamma_E}(\gamma_E) = 1 - e^{-\frac{\gamma_E}{\overline{\gamma}_E}}. \tag{7}$$

III. On-Off Transmission Scheme with Statistical Knowledge on the Eavesdropper's Channel

In this section, we reveal two fundamental properties of the OOT scheme by assuming the average SNR of the eavesdropper's channel being available at Alice.

A. Preliminaries

In a wiretap channel, the secrecy capacity, C_s, is defined as

$$C_s = \begin{cases} C_B - C_E \ , & \gamma_B > \gamma_E \\ 0 \ , & \gamma_B \leq \gamma_E, \end{cases} \tag{8}$$

where $C_B = \log_2(1+\gamma_B)$ is the capacity of the main channel and $C_E = \log_2(1+\gamma_E)$ is the capacity of the eavesdropper's channel. According to the definition of C_s, the hybrid secrecy outage probability is given by

$$P_{hso}(R_s) = \Pr(C_s < R_s). \tag{9}$$

In the OOT scheme, R_s is fixed as a constant and Alice only transmits when $C_B > R_s$. As such, Bob can always decode a message in case of a transmission, i.e., the reliability constraint is guaranteed for every transmission. The probability that Alice transmits a signal (i.e., transmission probability) within the OOT scheme is expressed as

$$P_{tx}(R_s) = \Pr(C_B > R_s) = \Pr(\gamma_B > 2^{R_s} - 1). \tag{10}$$

The conditional secrecy outage probability, which is defined as the probability that the redundance rate, $(C_B - R_s)$, is less than C_E in case of transmission, can be expressed as

$$\begin{aligned} P_{cso}(R_s) &= \Pr(C_B - R_s < C_E | R_s < C_B) \\ &= \frac{\Pr(2^{R_s} - 1 < \gamma_B < 2^{R_s}(1+\gamma_E) - 1)}{\Pr(\gamma_B > 2^{R_s} - 1)}. \end{aligned} \tag{11}$$

B. Transmission Probability and Two Secrecy Outage Probabilities of the On-Off Transmission Scheme

The hybrid secrecy outage probability of a wiretap channel can be expressed as a function of the transmission probability and the conditional secrecy outage probability of the OOT scheme, which is provided in the following theorem.

***Theorem** 1:* The expression of $P_{hso}(R_s)$ as a function of $P_{tx}(R_s)$ and $P_{cso}(R_s)$ is given by

$$P_{hso}(R_s) = 1 - P_{tx}(R_s)\left[1 - P_{cso}(R_s)\right]. \tag{12}$$

Proof: Following (9), $P_{hso}(R_s)$ can be rewritten as

$$\begin{aligned} P_{hso}(R_s) = {} & \Pr(C_s < R_s | \gamma_B > \gamma_E) \Pr(\gamma_B > \gamma_E) \\ & + \Pr(C_s < R_s | \gamma_B < \gamma_E) \Pr(\gamma_B < \gamma_E). \end{aligned} \tag{13}$$

Since $C_s = 0$ for $\gamma_B < \gamma_E$ and $R_s \geq 0$, we have $\Pr(C_s < R_s | \gamma_B < \gamma_E) = 1$. Then, following (13) we have

$$\begin{aligned} P_{hso}(R_s) &= \Pr\left[\gamma_E < \gamma_B < 2^{R_s}(1+\gamma_E) - 1\right] + \Pr(\gamma_B < \gamma_E) \\ &= \Pr\left[0 < \gamma_B < 2^{R_s}(1+\gamma_E) - 1\right]. \end{aligned} \tag{14}$$

Following (10) and (11), we have

$$P_{tx}(R_s)\left[1 - P_{cso}(R_s)\right] = \Pr\left[2^{R_s}(1+\gamma_E) - 1 < \gamma_B\right]. \tag{15}$$

Comparing (14) and (15), we obtain

$$P_{hso}(R_s) = 1 - P_{tx}(R_s)\left[1 - P_{cso}(R_s)\right] \tag{16}$$

$$= \left[1 - P_{tx}(R_s)\right] + P_{tx}(R_s) P_{cso}(R_s). \tag{17}$$

This completes the proof. ∎

We note that Theorem 1 clarifies, for the first time, that the hybrid secrecy outage probability can be achieved by the OOT scheme in a wiretap channel and also indicates that the hybrid secrecy outage probability is a practical and meaningful performance metric. It can be seen from (17) that the hybrid secrecy outage probability incorporates the transmission outage probability, $1 - P_{tx}(R_s)$, and the secrecy outage probability in case of all possible transmissions, $P_{tx}(R_s)P_{cso}(R_s)$. Based on the proof of Theorem 1, we note that (12) is independent of the specific statistical information of the main channel and the eavesdropper's channel, i.e., (12) is valid for any pdfs of γ_B and γ_E.

C. Lower Bound on the Strict Secrecy Outage Probability of the On-Off Transmission Scheme

In case of transmission, the conditional secrecy outage probability of the OOT scheme is larger than a specific value ϵ, which is solely determined by $\overline{\gamma}_B$ and $\overline{\gamma}_E$ and is derived in the following theorem.

***Theorem** 2:* The lower bound on the conditional secrecy outage probability of the OOT scheme is derived as

$$\epsilon = \frac{\overline{\gamma}_E}{\overline{\gamma}_B + \overline{\gamma}_E}. \tag{18}$$

Proof: Following (11), the conditional secrecy outage probability of the OOT scheme can be rewritten as

$$\begin{aligned} P_{cso}(R_s) = \int_0^\infty & \frac{F_{\gamma_B}(2^{R_s}(1+\gamma_E) - 1) - F_{\gamma_B}(2^{R_s} - 1)}{1 - F_{\gamma_B}(2^{R_s} - 1)} \\ & \times f_{\gamma_E}(\gamma_E) d\gamma_E. \end{aligned} \tag{19}$$

Substituting (3) and (6) into (19), we obtain

$$P_{cso}(R_s) = 1 - \frac{1}{\overline{\gamma}_E} \int_0^\infty e^{-\left(\frac{\overline{\gamma}_B + 2^{R_s}\overline{\gamma}_E}{\overline{\gamma}_B \overline{\gamma}_E}\right)\gamma_E} d\gamma_E. \tag{20}$$

We then solve the integral in (20) by using $\int_0^\infty e^{-\mu x} dx = \mu^{-1}$, which results in

$$P_{cso}(R_s) = \frac{2^{R_s}\overline{\gamma}_E}{\overline{\gamma}_B + 2^{R_s}\overline{\gamma}_E} \tag{21}$$

Based on (21) we know that $P_{cso}(R_s)$ is a monotonically increasing function of R_s. As such, the minimum value of $P_{cso}(R_s)$ is achieved as given in (18) for $R_s = 0$. This completes the proof. ∎

We note that Theorem 2 demonstrates that in the OOT scheme in case of transmission $P_{cso}(R_s)$ is bounded by ϵ and we cannot achieve an arbitrary small secrecy outage probability by varying R_s. It can be seen from (18) that the lower bound on $P_{cso}(R_s)$ is solely determined by the average SNRs of the main channel and the eavesdropper's channel. Specifically, ϵ is a monotonically decreasing function of $\overline{\gamma}_B$ and a monotonically increasing function of $\overline{\gamma}_E$.

IV. On-Off Transmission Scheme within an Absolutely Passive Eavesdropping Scenario

In this section, we examine the OOT scheme within an completely passive eavesdropping scenario, in which even the average SNR of the eavesdropper's channel is unavailable at Alice. Specifically, we derive an expression for conditional secrecy outage probability in the completely passive eavesdropping scenario, where the eavesdropper's location is uniformly distributed in an annulus.

A. Preliminaries (Annulus Threat Model)

In the annulus threat model, the annulus is bounded by two concentric circles, where ρ_i and ρ_o are the radii of the inner circle and the outer circle, respectively, Alice is assumed to be at the center of the two concentric circles, and the distance between Alice and Eve is denoted as ρ. Without other statements, all distances in this work are in meters. As discussed in [14], ρ_i and ρ_o can be known based on the physical location of Alice and a SNR threshold. Adopting the path loss model, the average SNR of the eavesdropper's channel can be expressed as a function of ρ, which is given by [15]

$$\overline{\gamma}_E = c_0 \rho^{-\eta}, \tag{22}$$

where $c_0 = \overline{\gamma}_0 / \rho_r^{-\eta}$, $\overline{\gamma}_0$ is the reference average SNR of the eavesdropper's channel at the reference distance ρ_r, and η is the path loss exponent. In this work, we assume that c_0, ρ_r, and η are publicly known, which can be estimated through a priori

measurement campaigns in the vicinity of Alice. As proved in [14], the square of the distance between Alice and Eve, ρ^2, follows a uniform distribution with ρ_i^2 and ρ_o^2 as the lower bound and upper bound, respectively, i.e., $\rho^2 \sim \mathbf{U}(\rho_i^2, \rho_o^2)$.

B. Average Conditional Outage Probability of the On-Off Transmission scheme

From Theorem 1 we know that the hybrid secrecy outage probability of the OOT scheme can be expressed as a function of its transmission probability and conditional secrecy outage probability. Given that the transmission probability of the OOT scheme is not a function of $\overline{\gamma}_E$, in this subsection we focus on deriving the average conditional secrecy outage probability of the OOT scheme within the annulus threat model, which is provided in the following theorem.

***Theorem** 3:* The average conditional secrecy outage probability, $\overline{P}_{cso}(R_s)$, of the OOT scheme within the annulus threat model is derived as

$$\overline{P}_{cso}(R_s) = 1 - \frac{\rho_o^2}{\rho_o^2 - \rho_i^2} {}_2F_1\left(1, -\frac{2}{\eta}; 1 - \frac{2}{\eta}; -\frac{2^{R_s} c_0 \rho_o^{-\eta}}{\overline{\gamma}_B}\right) + \frac{\rho_i^2}{\rho_o^2 - \rho_i^2} {}_2F_1\left(1, -\frac{2}{\eta}; 1 - \frac{2}{\eta}; -\frac{2^{R_s} c_0 \rho_i^{-\eta}}{\overline{\gamma}_B}\right), \quad (23)$$

where ${}_2F_1(\cdot,\cdot;\cdot;\cdot)$ denotes the Gauss hypergeometric function, which is given by

$${}_2F_1(a, b; c; z) = \sum_{n=0}^{\infty} \frac{(a)_n (b)_n z^n}{(c)_n n!}, \quad (24)$$

and $(\cdot)_n$ for nonnegative integers n is given by

$$(\alpha)_n = \begin{cases} 1 \ , & n = 0, \\ \alpha(\alpha+1)\cdots(\alpha+n-1) \ , & n \geq 1. \end{cases} \quad (25)$$

Proof: The average conditional secrecy outage probability is obtained by averaging the conditional secrecy outage probability over all possible locations of Eve within the annulus threat model, which is given by

$$\overline{P}_{cso}(R_s) = \int_{\rho_i^2}^{\rho_o^2} \frac{P_{cso}(R_s)}{\rho_o^2 - \rho_i^2} d\rho^2 \quad (26)$$

Substituting (21) into (26), we have

$$\begin{aligned} \overline{P}_{cso}(R_s) &= \frac{1}{\rho_o^2 - \rho_i^2} \int_{\rho_i^2}^{\rho_o^2} \left(1 - \frac{\overline{\gamma}_B}{\overline{\gamma}_B + 2^{R_s} \overline{\gamma}_E}\right) d\rho^2 \\ &= 1 - \frac{1}{\rho_o^2 - \rho_i^2} \int_{\rho_i^2}^{\rho_o^2} \frac{1}{1 + \frac{2^{R_s} c_0}{\overline{\gamma}_B} (\rho^2)^{-\frac{\eta}{2}}} d\rho^2 \end{aligned} \quad (27)$$

We then solve the integral in (27) with the aid of [16, Eq. (9.100)] and obtain the result in (23) after some algebraic manipulations. ■

We note that the Gauss hypergeometric function ${}_2F_1(\cdot,\cdot;\cdot;\cdot)$ is available in MATLAB, and thus our derived average conditional secrecy outage probability $\overline{P}_{cso}(R_s)$ can be efficiently evaluated. Noting (12) and that the transmission probability $P_{tx}(R_s)$ is not a function of Eve's location, the average hybrid secrecy outage probability, $\overline{P}_{hso}(R_s)$, can be easily expressed as a function of $\overline{P}_{cso}(R_s)$ and $P_{tx}(R_s)$, which is given by

$$\overline{P}_{hso}(R_s) = 1 - P_{tx}(R_s)\left[1 - \overline{P}_{cso}(R_s)\right]. \quad (28)$$

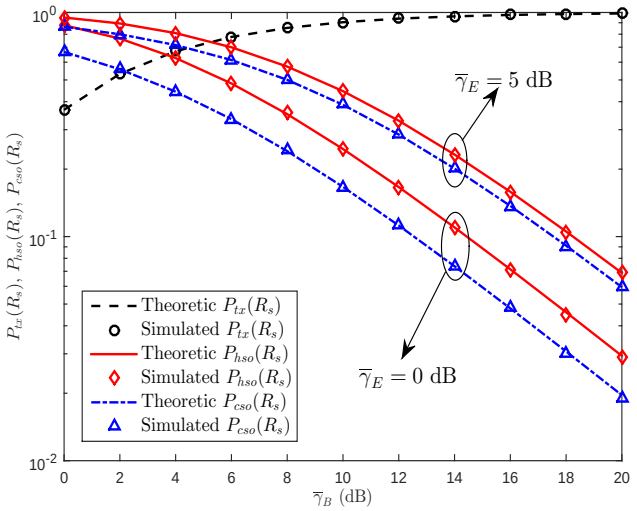

Fig. 2. Transmission probability $P_{tx}(R_s)$, hybrid secrecy outage probability $P_{hso}(R_s)$, and conditional secrecy outage probability $P_{cso}(R_s)$ of the OOT scheme versus $\overline{\gamma}_B$ for $R_s = 1$ and different values of $\overline{\gamma}_E$.

V. Numerical Results

In this section, we present numerical results to very our analysis and draw useful insights on our observations. Without other statements, we present the specific parameters adopted in our simulation in the caption of each figure.

In Fig. 2, we plot the theoretic and simulated transmission probability $P_{tx}(R_s)$, hybrid secrecy outage probability $P_{hso}(R_s)$, and conditional secrecy outage probability $P_{cso}(R_s)$ of the OOT scheme. In Fig. 2, the theoretic $P_{hso}(R_s)$ is calculated based on Theorem 1 and the simulated $P_{hso}(R_s)$ is numerically calculated based on (9) with thousands of channel realizations. In this figure, we first observe that the simulated $P_{hso}(R_s)$ precisely matches the theoretic $P_{hso}(R_s)$, which confirms our analysis provided in Theorem 1. We also observe that the simulated $P_{tx}(R_s)$ and $P_{cso}(R_s)$ match the theoretic $P_{tx}(R_s)$ and $P_{cso}(R_s)$, respectively. This confirms the correctness of (10) and (21). Furthermore, we observe that the hybrid secrecy outage probability is always larger than the secrecy secrecy outage probability and the gap between them decreases as $\overline{\gamma}_E$ increases, which can be explained by (17).

In Fig. 3 we plot the conditional secrecy outage probability for different values of R_s and its lower bound ϵ. As expected, we first observe that $P_{cso}(R_s)$ approaches ϵ as R_s approaches zero and once R_s is lower than 0.1 the conditional secrecy outage probability is very close to ϵ. This confirms the correctness of our Theorem 2. We also observe that both $P_{cso}(R_s)$ and ϵ decreases as $\overline{\gamma}_B$ increases and increases as $\overline{\gamma}_E$ increases.

In Fig. 4 we plot the average hybrid secrecy outage probability $\overline{P}_{hso}(R_s)$ and average conditional secrecy outage

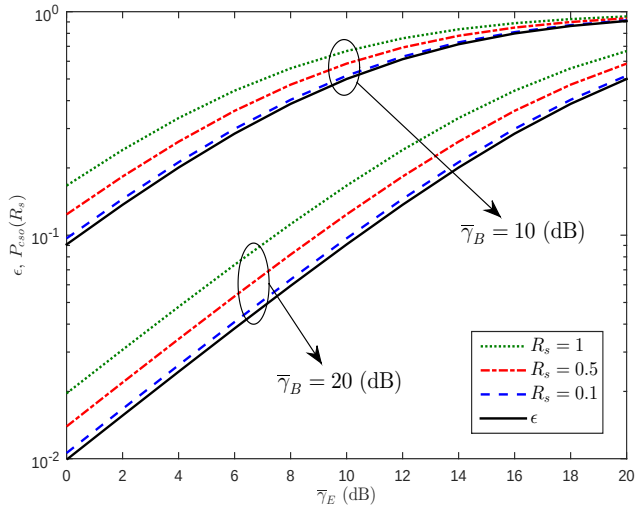

Fig. 3. Strict secrecy outage probability $P_{cso}(R_s)$ and ϵ of the OOT scheme versus $\overline{\gamma}_E$ for different values of $\overline{\gamma}_B$ and R_s.

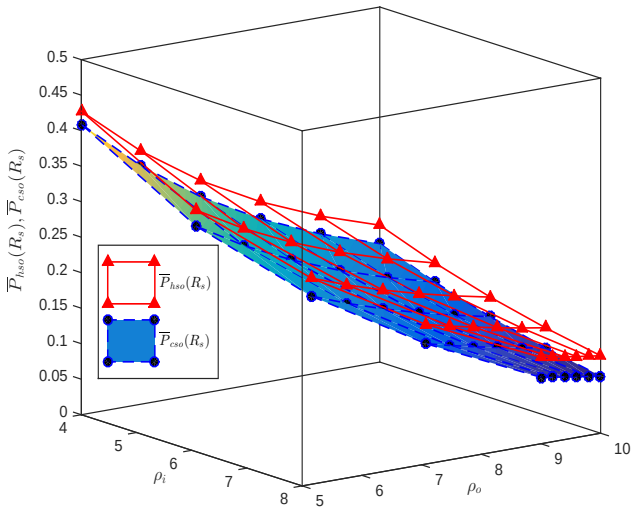

Fig. 4. Average hybrid secrecy outage probability $\overline{P}_{hso}(R_s)$ and average conditional secrecy outage probability $\overline{P}_{cso}(R_s)$ of the OOT scheme versus ρ_i and ρ_o for $\overline{\gamma}_B = 15$dB, $\eta = 3$, $\overline{\gamma}_0 = 30$dB, $\rho_r = 1$, and $R_s = 1$.

probability $\overline{P}_{cso}(R_s)$ of the OOT scheme within the annulus threat model. In the preparation of this figure, we also conduct simulations to verify our theoretic analysis. As expected, the simulation results precisely match our theoretic analysis, which confirms the correctness of our Theorem 3. To avoid cluttering, we omit the simulation points in this figure. We first observe that both $\overline{P}_{hso}(R_s)$ and $\overline{P}_{cso}(R_s)$ decrease as ρ_i increases. This can be explained by the fact that $P_{cso}(R_s)$ decreases as Eve moves away from Alice for fixed $\overline{\gamma}_B$, since $\overline{\gamma}_E$ decreases as each ρ increases. In addition, we observe that both $\overline{P}_{hso}(R_s)$ and $\overline{P}_{cso}(R_s)$ also decrease as ρ_o increases. This is mainly due to the adopted annulus threat model, in which Eve's location is uniformly distributed in the annulus and thus as ρ_o increases the distance between Eve and Alice increases on average.

VI. Conclusion

In this work, we first revealed two fundamental properties of the OOT scheme. The first one is that the widely used hybrid secrecy outage probability can be expressed as a function of the transmission probability and the conditional secrecy outage probability of the OOT scheme. This is the first time to relate the hybrid secrecy outage probability with a practical transmission scheme in wiretap channels. The second one is that in the OOT scheme we cannot achieve an arbitrary small conditional secrecy outage probability through varying the secrecy rate and the lower bound on this conditional secrecy outage probability is determined by the average SNRs of the main channel and the eavesdropper's channel. Adopting the annuls threat model, we then derived an expression for the average conditional secrecy outage probability of the OOT scheme, which can be evaluated efficiently.

Acknowledgement

This work was supported by the Australian Research Council under Discovery Projects grant DP150103905.

References

[1] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for secrecy in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[2] H. Wang, X. Zhou, and M. Reed, "Physical layer security in cellular networks: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2776–2787, May 2013.

[3] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20-27, Apr. 2015.

[4] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Techn. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[5] A. Wyner, "The wire-tap channel," *Bell Syst. Techn. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[6] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[7] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[8] X. Zhou, M. R. McKay, B. Maham, and A. Hjørungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.

[9] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372–375, Jun. 2012.

[10] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Jan. 2013.

[11] S. Yan, N. Yang, R. Malaney, and J. Yuan, "Transmit antenna selection with Alamouti coding and power allocation in MIMO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1656–1667, Mar. 2014.

[12] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.

[13] S. Yan, N. Yang, R. Malaney, and J. Yuan, "Full-duplex wiretap channels: security enhancement via antenna switching," in *Proc. IEEE GlobeCOM TCPLS Workshop*, Dec. 2014, pp. 1412–1417.

[14] S. Yan, N. Yang, G. Geraci, R. Malaney, and J. Yuan, "Optimization of code rates in SISOME wiretap channels," *IEEE Trans. Wireless Commun.*, accepted to appear, Jul. 2015.

[15] A. Goldsmith, *Wireless Communications*, Cambridge, U.K.: Cambridge Univ. Press, 2005.

[16] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 7th ed., Academic, San Diego, CA, 2007.